



STABILIZING GLOBAL DATA INTEGRITY AND PERFORMANCE AFTER A MAJOR INFRASTRUCTURE MIGRATION

Zero

DATA INGESTION LAG

100%

DLQ ISOLATION

90%

TRIAGE TIME REDUCTION

CLIENT

A prominent US IT services provider undergoing a massive global infrastructure and log management migration.

GEO: USA



IT Services & Consulting

PROJECT CONTEXT

- Modernized an enterprise log management infrastructure by remediating critical post-migration issues after a migration from Splunk to Elastic.
- Resolved severe operational hurdles, including regional data synchronization lag and potential data loss.
- Successfully stabilized the environment and secured uninterrupted data integrity while transitioning complex monitoring workflows to the new architecture.

PROJECT OBJECTIVES

- Resolve reported data loss and enrichment gaps to maintain a reliable source of truth.
- Mitigate root causes of data lag occurring between local agents and the central cluster.
- Replicate legacy dashboard visualizations to ensure consistent business reporting.
- Implement real-time mechanisms to capture and analyze data ingestion failures.

SOLUTION DELIVERY

- **Diagnostic Analysis:** Analyzed system logs to distinguish between genuine data loss and duplicates caused by configuration filters.
- **Resilient Pipelines:** Established Dead Letter Queues (DLQ) to isolate failed records and prevent silent data loss.
- **Data Enrichment:** Developed logic to propagate event headers across multi-line documents, ensuring full traceability.
- **Reporting Realignment:** Provided specialized transformation configurations to handle complex data consolidation for dashboards.

TECHNOLOGY STACK



elasticsearch



logstash



KIBANA